831, 834 (Fed. Cir. 1990). The Examiner bears the initial burden of establishing a prima facie case of obviousness. *See* M.P.E.P. § 2142. To establish a prima facie case of obviousness, the Examiner must show, inter alia, that there is some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify or combine the references and that, when so modified or combined, the prior art teaches or suggest all of the claim limitations. *See* M.P.E.P. § 2143.

Applicants respectfully disagree with the Examiner that Robert in view of Misra renders claims 1 to 14 or 44 to 73 of the present application unpatentable.

Claim 1 recites the following:

> A method for controlling the use of a data object using encrypted network address information, comprising the steps of:
> *receiving a data object and encrypted network address information from a server;*
> playing the contents of said data object;
> *decrypting said encrypted network address information;*
> *determining whether said decrypted network address information corresponds to a network address of said server;* and
> if said correspondence does not exist, ceasing to play the contents of said data object.

Claim 44 recites the following:

> A method for controlling the playing of content using encrypted network address information, comprising the steps of:
> *receiving a data object and encrypted network address information from a server;*
> *decrypting said encrypted network address information;*
> *determining whether said decrypted network address information corresponds to a network address of said server;* and
> if said correspondence does exist, playing the contents of said data object.

Claim 60 recites the following:

> An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when

executed, define a series of steps to be used to control the playing of the contents of a data object, said steps comprising:

receiving a data object and encrypted network address information from a server;

decrypting said encrypted network address information;

determining whether said decrypted network address information corresponds to a network address of said server; and

if said correspondence exists, playing the contents of said data object.

Claims 2 to 14 depend from claim 1. Claims 45 to 59 depend from claim 44. Claims 61 to 73 depend from claim 60. Respectfully, neither Robert or Misra describe "receiving a data object and encrypted network address information from a server," "decrypting said encrypted network address information" or "determining whether said decrypted network address information corresponds to a network address of said server."

Robert describes a license management system where a license management facility maintains a value for the maximum number of licenses ("license unit value") and a value for the number of licenses allocated ("license usage allocation unit value"). The system of Robert issues licenses in response to requests and does not allow the number of allocated licenses to exceed the maximum number of licenses. *See* Col. 2:5-29. Robert does not describe any use of encrypted network address information.

Misra describes a system for licensing software where licenses are generated at a licensing clearinghouse and distributed to license servers in digitally signed "license packs." The license servers then distribute digitally signed licenses to client computers that have requested them. *See* Col. 2:11-25. Misra does not describe any use of encrypted network address information.

In contrast, certain embodiments of the present application, for example, use encrypted network address information to control a data object received from a server. Once received, the encrypted network address information is decrypted and compared to the address of the server from which it was received. If the address information does not match, use of the data object is not allowed or is only allowed in a limited form. Neither Robert or Misra describes using encrypted network address information to control the use of data objects.

Claims 2 to 14, 43 to 59 and 61 to 73 depend from claims 1, 44 and 60. Accordingly,

the arguments presented above in connection with claims 1, 44 and 60 apply equally to claims 2 to 14, 43 to 59 and 61 to 73. In view of the foregoing, it is submitted that neither Robert nor Misra, alone or combined, renders any of claims 1 to 14 or 44 to 73 obvious.

Thus, it is respectfully submitted that the rejection of claims 1 to 14 and 44 to 73 under 35 U.S.C. § 103 over Robert in view of Misra should be withdrawn.

Applicants also respectfully disagree with the Examiner that Robert in view of Misra renders claims 15 to 26 or 81 to 87 of the present application unpatentable.

Claim 15 recites the following:

> A method for controlling the playing of content using encrypted network address information, comprising the steps of:
>> *receiving a data object and encrypted network address information from a first server;*
>> playing the contents of said data object;
>> *decrypting said encrypted network address information;*
>> *receiving a plurality of network addresses from a second server corresponding to said decrypted network address information;*
>> *searching said plurality of network addresses for a network address of said first server;* and
>> if said search fails, ceasing to play the contents of said data object.

Claim 81 recites the following:

> An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to be used to control the playing of the contents of a data object, said steps comprising:
>> *receiving a data object and encrypted network address information from a first server;*
>> playing the contents of said data object;
>> *decrypting said encrypted network address information;*
>> *receiving a plurality of network addresses from a second server corresponding to said decrypted network address information;*
>> *searching said plurality of network addresses for a network address of said first server;* and
>> if said search fails, ceasing to play the contents of said

data object.

Claims 16 to 26 depend from claim 15. Claim 82 to 87 depend from claim 81. Respectfully, as explained above, neither Robert or Misra describe "receiving a data object and encrypted network address information from a first server" or "decrypting said encrypted network address information." Furthermore, neither Robert or Misra describe "receiving a plurality of network addresses from a second server corresponding to said decrypted network address information" and "searching said plurality of network addresses for a network address of said first server."

In contrast, certain embodiments of the present invention, for example, use encrypted network address information to control a data object received from a first server. Once received, the encrypted network address information is decrypted and a list of network addresses is received from a second server, the second server corresponding to the decrypted network address information. This list of network addresses is then compared to the address of the first server from which the data object was received. If the first server's address information is not found in the list, use of the data object is not allowed or is only allowed in a limited form. Neither Robert or Misra describes using encrypted network address information in this way to control the use of data objects.

Claims 16 to 26 and 82 to 87 depend from claims 15 and 81. Accordingly, the arguments presented above in connection with claims 15 and 81 apply equally to claims 16 to 26 and 82 to 87. In view of the foregoing, it is submitted that neither Robert nor Misra, alone or combined, renders any of claims 15 to 26 or 81 to 87 obvious.

Thus, it is respectfully submitted that the rejection of claims 15 to 26 and 81 to 87 under 35 U.S.C. § 103 over Robert in view of Misra should be withdrawn.

Applicants also respectfully disagree with the Examiner that Robert in view of Misra renders claims 27 to 33 or 74 to 80 of the present application unpatentable.

Claim 27 recites the following:

> A method for controlling the playing of content using encrypted network address information, comprising the steps of:
> > *receiving a data object and encrypted network address information from a server;*
> > playing the contents of said data object;
> > *decrypting said encrypted network address*

information;
   searching a plurality of network addresses for a
network address corresponding to said decrypted network
address information; and
   if said search succeeds, ceasing to play the contents of
said data object.

Claim 74 recites the following:

  An article of manufacture comprising a computer-readable
medium having stored thereon instructions adapted to be
executed by a processor, the instructions which, when
executed, define a series of steps to be used to control the
playing of the contents of a data object, said steps comprising:
   receiving a data object and encrypted network address
information from a server;
   playing the contents of said data object;
   decrypting said encrypted network address
information;
   searching a plurality of network addresses for a
network address corresponding to said decrypted network
address information; and
   if said search succeeds, ceasing to play the contents of
said data object.

Claims 28 to 33 depend from claim 27. Claims 75 to 80 depend from claim 74.
Respectfully, as explained above, neither Robert or Misra describe "receiving a data object
and encrypted network address information from a server" or "decrypting said encrypted
network address information." Furthermore, neither Robert or Misra describe "searching a
plurality of network addresses for a network address corresponding to said decrypted network
address information."

In contrast, certain embodiments of the present invention, for example, use encrypted
network address information to control a data object received from a server. Once received,
the encrypted network address information is decrypted and compared to a list of network
addresses. If the server's address information is found in the list, use of the data object is not
allowed or is only allowed in a limited form. Neither Robert or Misra describe using
encrypted network address information in this way to control the use of data objects.

Claims 28 to 33 and 75 to 80 depend from claims 27 and 74. Accordingly, the
arguments presented above in connection with claims 27 and 74 apply equally to claims 28 to

-6-

33 and 75 to 80. In view of the foregoing, it is submitted that neither Robert nor Misra, alone or combined, renders any of claims 27 to 33 or 74 to 80 obvious.

Thus, it is respectfully submitted that the rejection of claims 27 to 33 and 74 to 80 under 35 U.S.C. § 103 over Robert in view of Misra should be withdrawn.

Applicants also respectfully disagree with the Examiner that Robert in view of Misra renders claims 34 to 43, 88 or 89 of the present application unpatentable.

Claim 34 recites the following:

> A method for calculating license fees for client software based on the network address of the content provider, comprising the steps of:
> *receiving a plurality of records from a plurality of software clients wherein each record includes a network address;*
> *determining the number of records of said plurality of records that include a particular network address; and*
> *calculating a license fee for said particular network address based on said number of records.*

Claim 39 recites the following:

> A system for calculating software licensing fees, comprising:
> a plurality of software clients;
> a plurality of content servers; and
> a billing server,
> wherein each of said plurality of software clients downloads and plays content from said plurality of content servers, *logs information about the content played, and sends said logged information to said billing server*; and said billing server *uses the logged information received from said plurality of software clients to calculate the number of times that content from each content server was played and uses said number of times to calculate a license fee to be charged to the entity that operates the content server.*

Claim 88 recites the following:

> An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to be used to calculate license fees for client software based on the network address of the content provider, said steps comprising:
> *receiving a plurality of records from a plurality of software clients wherein each record includes a network*

-7-

address;

> *determining the number of records of said plurality of records that include a particular network address; and*
>
> *calculating a license fee for said particular network address based on said number of records.*

Claims 35 to 38 depend from claim 34. Claims 40 to 43 depend from claim 39. Claim 89 depends from claim 88. Respectfully, neither Robert or Misra describe "receiving a plurality of records from a plurality of software clients wherein each record includes a network address," "determining the number of records of said plurality of records that include a particular network address" or "calculating a license fee for said particular network address based on said number of records." Nor does Robert or Misra describe software clients "log[ging] information about the content played, and send[ing] said logged information to said billing server" and a billing server "us[ing] the logged information received from said plurality of software clients to calculate the number of times that content from each content server was played and us[ing] said number of times to calculate a license fee to be charged to the entity that operates the content server."

In contrast, in certain embodiments of the present invention, for example, software clients log information about content they have downloaded/played from a content server and send that information to a billing server. The billing server then uses this information to calculate how many times content from each content server was downloaded/played and calculates a corresponding license fee to be charged to the entity which operates the content server. This calculation may be made, for example, by counting the number of times the content server's network address appears in the logged information. Neither Robert or Misra describe using information logged by software clients and sent to a billing server to calculate licensing fees for content providers.

Claims 35 to 38, 40 to 43 and 89 depend from claims 34, 39 and 88. Accordingly, the arguments presented above in connection with claims 34, 39 and 88 apply equally to claims 35 to 38, 40 to 43 and 89. In view of the foregoing, it is submitted that neither Robert nor Misra, alone or combined, renders any of claims 34 to 43, 88 or 89 obvious.

Thus, it is respectfully submitted that the rejection of claims 34 to 43, 88 and 89 under 35 U.S.C. § 103 over Robert in view of Misra should be withdrawn.

Applicants also respectfully disagree with the Examiner that Robert in view of Misra

renders claims 90 to 97 of the present application unpatentable.

Claim 90 recites the following:

A method for controlling the use of a data object using network address information, comprising the steps of:
receiving a data object and network address information from a server;
playing the contents of said data object;
sending a message to a verification server containing said network address information;
receiving a response from said verification server; and
if said response is negative, ceasing to play the contents of said data object.

Claims 91 to 97 depend from claim 90. Respectfully, neither Robert or Misra describe "receiving a data object and network address information from a server" and "sending a message to a verification server containing said network address information." In contrast, certain embodiments of the present invention control the use of data objects by, for example, sending a message to a verification server including network address information received with the data object, and awaiting a message from the verification server verifying that the network address information belongs to a licensed content provider. Neither Robert or Misra describes using network address information and a message to a verification server to control the use of data objects.

Claims 91 to 97 depend from claim 90. Accordingly, the arguments presented above in connection with claim 90 apply equally to claims 91 to 97. In view of the foregoing, it is submitted that neither Robert nor Misra, alone or combined, renders any of claims 90 to 97 obvious.

Thus, it is respectfully submitted that the rejection of claims 90 to 97 under 35 U.S.C. § 103 over Robert in view of Misra should be withdrawn.

Conclusion

It is respectfully submitted that the application is in condition for allowance, and Applicants request reconsideration and withdrawal of all grounds of rejection.

A Notice of Allowance is respectfully requested.

The Office is hereby authorized to charge any additional fees or credit any overpayments under 37 C.F.R. §1.16 or §1.17 to Deposit Account No. 11-0600.
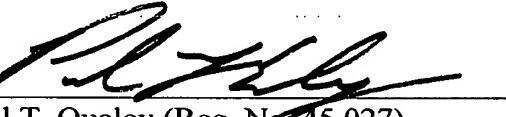
The Examiner is invited to contact the undersigned at (212) 425-7200 to discuss the application.

Respectfully submitted,

Dated: **2/4/03**

By: _____
Paul T. Qualey (Reg. No. 45,027)
KENYON & KENYON
One Broadway
New York, N.Y. 10004
(212) 425-7200 (telephone)
(212) 425-5288 (facsimile)

549880